MN128-SOHO
IB3

ファームウェア バージョン 1.30 追加説明

この度は、MN128-SOHO IB3をお買い上げいただき、誠にありがとうございます。
MN128-SOHO IB3のマニュアルに追加説明事項があります。
本製品をご使用になる前に、マニュアルとあわせてこの追加説明書をお読みください。

追加説明事項

◎『導入/設定ガイド』(製品付属マニュアル)への追加事項

●NATセッション数の増加

従来は接続相手先ごとに256セッションまででしたが、全体で4096セッションまで可能になりました。また、ステートフル・パケット・インスペクションで対応するセッション数も増えています。

●FAXの無鳴動着信機能に対応 ☞〈P.2〉

本製品のTELポートに、無鳴動着信対応のFAXを接続すると、呼び出し音なしで受信することができます。これを「サイレントFAX」機能と呼びます。

●電話の呼び出し音を切り替えられます ☞〈P.3〉

外線が着信したときの呼び出し音を、ポートごとに切り替えられます。

●通話中、他の相手に電話をかけられます(通話中発信) ☞〈P.4〉

通話中、通話している相手を保留にし、他の相手に電話をかけることができます。INSネット64のフレックスホンの、三者通話機能と同じような機能です。

◎『活用ガイド〜初級編』(WEB公開マニュアル)への追加事項

●Messengerでの電話による通話に対応 ☞〈P.6〉

Windows Messenger/MSN Messengerで、電話がかけられます。

◎『活用ガイド〜中・上級編』(WEB公開マニュアル)への追加事項

●指定したTELポートからの発信を禁止できます ☞〈P.7〉

指定したTELポートからの発信を一切禁止できます。緊急電話番号(110、118、119、171)のみ発信を許可することもできます。

●不正なアクセスを検知し、防御することができます(DoS攻撃防御) ☞〈P.8〉

DoS攻撃防御機能により、不正なアクセスを検知し、LAN側のネットワークを保護します。

◎『リファレンス・ハンドブック』(WEB公開マニュアル)への追加事項

●フッキングなしで設定できるようにする機能、および、指定したTELポートの電話機から設定できないようにする機能を追加 ☞〈P.15〉

フッキングなしで直接設定できるようにしたり、そのTELポートから設定できないようにします。

●アナログクイック設定機能を追加 ☞〈P.17〉

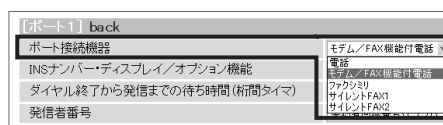
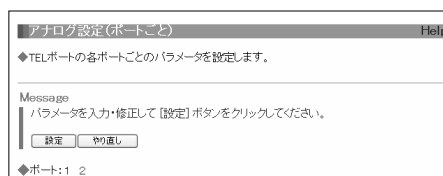
電話機からの設定コードのうち、よく使用されるものをまとめて簡単に設定する機能です。

FAXで無鳴動着信機能を使用する（サイレントFAX）

本製品のTELポートに、無鳴動着信対応のFAXを接続すると、呼び出し音なしで受信することができます。これを「サイレントFAX」機能と呼びます。

※FAX機が無鳴動着信（Fネットサービス）に対応していなければなりません。

※ナンバー・ディスプレイ、キャッチホン・ディスプレイ、ネーム・ディスプレイに対応しているFAXをお使いの場合、サイレントFAX機能を併用することはできません。同時に設定した場合、サイレントFAX機能が優先されます。

サイレントFAXを設定します

1 詳細設定ページの［アナログ設定］→［ポートごと］をクリックして、［アナログ設定（ポートごと）］画面を開きます。

2 接続したポートの［ポート接続機器］から、次のどちらかの項目を選択します。

サイレントFAX1：相手先がISDN回線を通じてFAXを送信してきたときのみ、FAXの呼び出し音が無音になります。

サイレントFAX2：常に呼び出し音が無音になります。

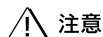
3 ［設定］ボタンをクリックします。

One Point!

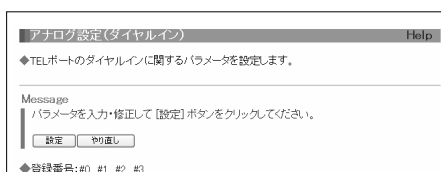
◇ATコマンド、設定コードは以下のようになります（サイレントFAX1/2は、n=3/4）

ATコマンド	AT@Er=n[p]
設定コード	32rn[p]
パラメータ	r=1～2　ポート番号 n=0　電話 n=1　モデム/FAX機能付電話 n=2　ファクシミリ n=3　サイレントFAX1 n=4　サイレントFAX2 p=0　ナンバー・ディスプレイ、キャッチホン・ディスプレイ、ネーム・ディスプレイを使用しない p=1　ナンバー・ディスプレイのみ使用する p=2　ナンバー・ディスプレイ、キャッチホン・ディスプレイを使用する p=3　ナンバー・ディスプレイ、キャッチホン・ディスプレイ、ネーム・ディスプレイを使用する

電話の呼び出し音を変更する

本製品では、ダイヤルイン登録番号０〜３のそれぞれについて、外線が着信したときの呼び出し音を設定することができます。

> ⚠ 注意
>
> TEL ポートに FAX やモデムをつないでいる場合、呼び出し音を変更すると着信できなくなることがあります。その場合は、［呼び出し音 1］に戻してください。

外線が着信したときの呼び出し音を設定します

1 詳細設定ページの［アナログ設定］→［ダイヤルイン］をクリックし、［アナログ設定（ダイヤルイン）］画面を開きます。

2 番号を登録した［ダイヤルイン登録番号］の、設定したいポートの［外線呼び出し音］で、呼び出し音の種類を選択します。

呼び出し音１：“リーン･リーン”（導入時の設定）

呼び出し音２：“リーンリン･リーンリン”

呼び出し音３：“リンリンリン･リンリンリン”

無鳴動：呼び出し音が鳴りません

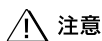
3 ［設定］ボタンをクリックします。

One Point!

◇ AT コマンド、設定コードは以下のようになります

ATコマンド	ＡＴ＠Ｍｑｒ＝ｎ
設定コード	６１ｑｒｎ
パラメータ	q=0 〜３ ダイヤルイン登録番号 r=1 〜２ ポート番号 n=**0** 呼び出し音１（リーン・リーン） n=1 呼び出し音２（リーンリン・リーンリン） n=2 呼び出し音３（リンリンリン・リンリンリン） n=3 無鳴動着信（1300Hz の無鳴動で着信）

通話中、他の相手に電話をかける（通話中発信）

NTT と契約していなくても、INS ネット64のフレックスホンの、三者通話（切り替えモードのみ）と同じような機能を使用することができます。
通話中、通話相手を保留にして、他の相手に電話をかけることができます。
この機能を「通話中発信」または「擬似三者通話」と呼びます。

注意

- この機能は、電話以外のアナログ機器では使用できません。
- この機能を使用する設定にすると、内線転送できなくなります。
- この機能を使用する設定にすると フレックスホンサービスのキャッチホン（コールウェイティング）、三者通話、通信中転送を利用できません。

通話中発信（擬似三者通話）を設定します

1 詳細設定ページの［アナログ設定］→［ポート共通］をクリックし、［アナログ設定（ポート共通）］画面を表示させせます。

2 ［擬似フレックスホン］の［通話中発信］で「する」を選択します。

3 ［設定］ボタンをクリックします。

これで設定は完了です。
通話中発信の操作手順は、次のページをお読みください。

One Point!

◇ AT コマンド、設定コードでは、擬似フレックスホンのほかの機能（マルチアンサー(擬似キャッチホン)、擬似着信転送）とまとめて設定します。

ATコマンド	ＡＴ＠０ｎ				
設定コード	６３ｎ				
パラメータ	n	通話中発信	マルチアンサー（擬似キャッチホン）	擬似着信転送	ご 注 意
	0				
	1		○		フレックスホンのキャッチホン（コールウェイティング）、三者通話、通信中転送は利用できません。
	2	○			
	3	○	○		
	4			○	フレックスホンの着信転送は利用できません。
	5		○	○	フレックスホンのすべての機能が利用できません。
	6	○		○	
	7	○	○	○	

通話中発信（擬似三者通話）をしてみましょう

1 通話中に、フックを１回押します。

受話器から“プップップッ”と聞こえます。

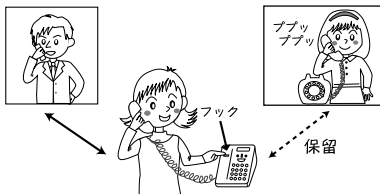
2 “プップップッ”と聞こえている間に、別の相手の電話番号をダイヤルします。

元の相手との通話は保留されます。保留されている相手側には、“ププッププッ”という保留音が聞こえます。

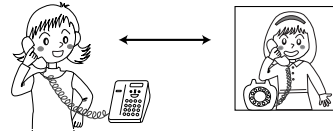
※別の相手の電話番号を間違えたとき、話し中などで相手が応答しないときは、一度受話器を置いてください。呼び出し音が鳴ります。受話器をとると、元の相手との通話に戻ります。

3 元の相手に戻りたいときは、フックを１回押します。

受話器から“プップップッ”と聞こえ、数秒後に元の相手と通話できるようになります。

もう片方の相手との通話は保留されます。

4 通話を終了したいときは、受話器を置きます。

通話していた相手との通話が切れ、呼び出し音が鳴ります。

5 受話器を上げると、保留されていた相手との通話に戻ります。

6 もう一度受話器を置くと、通話が終了します。

◇１つのTELポートでこの操作を行っている間は、他のTELポートで電話をかけたり受けたりすることはできません。

Messengerで電話をかけられます

本製品のUPnP（Universal Plug and Play：ユニバーサルプラグアンドプレイ）機能を利用すると、本製品のLANポートに接続したパソコンから、Windows Messenger4.7以上、またはMSN Messenger5.0以上を利用できます。本製品では、購入時にUPnP機能がONになっているので、とくに設定をする必要はありません。

※ 電話をかける機能を利用する際には、対応プロバイダとの契約が別途必要です。

※ Messengerを同時に利用できるパソコンは、４台までです。

※ UPnPを利用できるパソコンは、Windows XPおよびWindows Meです。
Windows Meの場合は、［コントロールパネル］→［アプリケーションの追加と削除］で［ユニバーサルプラグアンドプレイ］をインストールしてください。

※ Windows XPをご利用の場合は、［Windows Update］から［Service Pack1］と［重要な更新］のすべてをインストールしてください。

※ Windows Meをご利用の場合は、DirectX8.1以降をインストールしてください。また、［Windows Update］から［Service Pack1］と［重要な更新］のすべてをインストールしてください。

利用できる機能

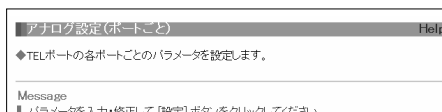
OS	Windows XP		Windows Me	
Messenger のバージョン	Windows Messenger 4.7, 5.0	MSN Messenger 5.0, 6.0	MSN Messenger 5.0	MSN Messenger 6.0
インスタントメッセージ	○	○	○	○
音声チャット	○	○	×※2	○※3
ビデオチャット	○	○	−	○※3
電話をかける	−※1	○	○	○
ファイル転送	×※2	○※3	○※3	○※3
アプリケーション共有	○	○	−	−
ホワイトボード	○	○	−	−
リモートアシスタンス	○	○	−	−
同一LAN内同士の音声チャット	○	○	○※3	○※3
同一LAN内同士のファイル送信	○	○	○※3	○※3
同一LAN内同士のビデオチャット	○	○	−	○※3
同一LAN内同士のアプリケーション共有	○	○	−	−
同一LAN内同士のホワイトボード	○	○	−	−

※１　Windows Messenger 4.7、5.0には、電話をかける機能は搭載されていません。
※２　バージョンアップで対応予定です。
※３　UPnP準拠の機能ではありませんが、本製品独自の機能によって利用できます。

指定したTEL ポートからの発信を禁止する

指定したTEL ポートに接続した機器から、発信できないように設定できます。
すべての発信を禁止することもできますが、緊急電話番号（110、118、119、171）の場合のみ発信を許可するようにもできます。

指定したTEL ポートからの発信を禁止する設定を行います

1 詳細設定ページの［アナログ設定］→［ポートごと］をクリックして、[アナログ設定（ポートごと)］画面を開きます。

2 ［オプション］欄をクリックして、次のコマンドを入力します。

※{ }で囲まれている部分はパラメータです。パラメータの区切りには、半角スペースを入力してください。

書式	analog call {port mode}
パラメータ	port = 1～2　ポート番号 mode　モード **allow**　すべての発信を許可する（購入時の設定） prohibit　すべての発信を禁止する sos　緊急電話番号以外への発信を禁止する

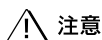
（例）TEL ポート２の電話機では、緊急電話番号以外への発信を禁止するとき

3 ［設定］ボタンをクリックします。

◇ AT コマンド、設定コードは以下のようになります

ATコマンド	AT#Pr=n
設定コード	74rn
パラメータ	r=1～2　ポート番号 n=**0**　すべての発信を許可する n=1　すべての発信を禁止する n=2　緊急電話番号以外の発信を禁止する

不正なアクセスを検知し、防御する（DoS 攻撃防御）

DoS 攻撃とは、正式にはDenial of Service（サービス拒否）攻撃と言います。ネットワークを通じて不正なデータを送信したり、大量にデータを送信したりすることにより、相手のサービスを使用不能にする攻撃です。
本製品では、DoS 攻撃防御機能により不正なアクセスを検知し、本製品およびLAN 側のネットワークを保護します。また、DoS 攻撃を検知したら、LAN の管理者など指定した相手先へメールを送信して通知できます。
導入時の設定では、DoS 攻撃防御機能はオフになっています。

⚠ 注意

● プライベートアドレスのネットワークを接続する場合

DoS 攻撃防御をオンにすると、IP Spoofing 攻撃（☞ 次ページ参照）防御の機能がオンになり、送信元のIP アドレスがプライベートアドレスのパケットが破棄されます。そのため、以下のような通信ができなくなる場合があります。

- ２拠点のプライベートアドレスネットワークをLAN 型で接続する場合
- 本製品のLAN 側で使用しているIP アドレスがプライベートアドレスで、リモートアクセスを受ける場合

この場合、該当する接続相手先のDoS 攻撃防御の設定をオフにしてご利用ください。
（☞「接続相手先ごとに、DoS 攻撃防御機能のON/OFF を設定する」〈P.14〉）

本製品で防御するDoS 攻撃について

- **FIN Scan**

  TCP FIN フラグがオンになっているパケットを送信して、ポートをスキャンします。
  本製品ではTCP 通信を監視し、パケットのFIN フラグが不正にオンになっているパケットを破棄します。

- **Null Scan**

  TCP フラグをすべてオフにしたパケットを送信して、ポートをスキャンします。
  本製品では、パケットのフラグをチェックし、すべてオフになっているパケットを破棄します。

- **Xmas Scan（Nmap Xmas Scan）**

  URG、PSH、FIN フラグがすべてオンのパケットを送信し、ポートをスキャンします。本製品では、上記のフラグをチェックし、すべてオンになっているパケットを破棄します。

- **Smurf 攻撃**

  送信元アドレスを偽造したICMP echo request パケットをブロードキャストすることにより、大量のICMP echo reply パケットを、相手先に返送させるという仕組みの攻撃です。
  本製品では、ブロードキャストアドレス宛てのICMP echo request パケットを破棄します。また、IP アドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。

- **Ping of Death 攻撃**

  Ping コマンドを使って不正なサイズのIP パケットを送信することにより、相手先の処理を不能にする攻撃です。
  本製品では、IP パケットのサイズをチェックして、不正なサイズのパケットを破棄します。

- **Teardrop 攻撃**

断片化されたIPパケット（IPフラグメンテーションパケット）を再構築する際の、TCP/IPの実装上の問題に対する攻撃です。IPフラグメンテーションパケットには、再構築時に使用されるオフセット情報が含まれますが、そのオフセット情報を偽造することで、相手先の処理を不能にします。
本製品では、オフセット情報をチェックし、同じオフセット番号のパケットを破棄することにより、そのIPアドレスからのセッションを遮断します。

- **IP Spoofing 攻撃**

送信元のIPアドレスを、相手先のIPアドレスに偽装することによる攻撃です。
本製品では、送信元のIPアドレスをチェックし、プライベートIPアドレスの場合、そのパケットを破棄します。

- **Land 攻撃**

送信元と送信先に同じIPアドレスを持つパケットを相手先に送信することにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。
本製品では、送信元と送信先のアドレスが同一かどうかをチェックし、同一のパケットを破棄します。

- **IP with Zero Length 攻撃**

IPパケットの最初のフラグメンテーションに、長さゼロのパケットを「おとり」として送信し、その後悪影響を及ぼすパケットを送り込むことで、相手先を攻撃します。
本製品では、パケットの最初のフラグメンテーションの長さ情報チェックし、ゼロの場合、そのパケットを破棄します。

- **Fraggle（UDP loop）**

送信元のIPアドレスを偽造し、UDPのecho requestパケットをブロードキャストすることにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。Echo、Chargen、Daytime、Qotdの各ポートが利用されます。
本製品では、ブロードキャストアドレス宛てのUDP echo requestパケットを破棄します。また、送信元のIPアドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。
また、送信元と送信先のポート番号が、7（Echo)、19（Chargen)、13（Daytime)、17（Qotd）の組み合わせである場合、そのパケットを破棄します。

- **Snork 攻撃**

送信先ポート番号が135、送信元ポート番号が7（Echo)、19（Chargen)、13（Daytime)、135のいずれかのUDPパケットを送信し、不正に処理を繰り返させる攻撃です。
本製品では、このようなパケットをすべて破棄します。

- **リロード攻撃**

Webページを連続してリロードすることにより、相手先に負荷を与える攻撃です。
本製品では、確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

- **Fragment Flood**

断片化されたパケットを大量に送信することにより、相手先を処理不能にする攻撃です。
本製品では、送信元のIPアドレスごとに、断片化されたパケット数をカウントし、設定した上限値を超えると、そのIPアドレスからのセッションを遮断します。

- **Connection Flood**

長時間オープン状態にし続けることにより、相手先のソケットを占拠する攻撃です。

本製品では、一定時間アイドル状態のまま確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

- **Ping Flooding**

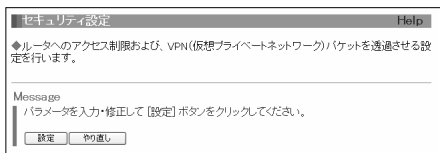
大量のICMP echo requestパケットを送信し、相手先のパフォーマンスを低下させる攻撃です。本製品では、ICMP echo requestパケット数をカウントし、設定した上限値を超えるとそのIPアドレスからのICMP echo requestパケットを破棄します。

- **SYN Flood**

SYNフラグがオンになっているTCPパケットを連続的に送信することにより、ハーフオープン状態のセッションを増加させ、相手先を処理不能にする攻撃です。
本製品では、SYNフラグがオンになっているTCPパケットの数、およびハーフオープン状態のセッション数をカウントし、設定した上限値を超えるとそのパケットを破棄します。

DoS攻撃防御機能をONにする

本製品でDoS攻撃防御機能を使用する場合は、次の手順で設定します。

1 詳細設定ページの［セキュリティ設定］をクリックして、［セキュリティ設定］画面を開きます。

2 ［DoS攻撃防御設定］の［DoS攻撃防御］で［する］を選択すると、以下のDoS攻撃が防御されます。

- FIN Scan
- Xmas Scan（Nmap Xmas Scan）
- Ping of Death攻撃
- IP Spoofing攻撃
- IP with Zero Length攻撃
- Snork攻撃
- Fragment Flood
- Ping Flooding
- Null Scan
- Smurf攻撃
- Teardrop攻撃
- Land攻撃
- Fraggle（UDP loop）
- リロード攻撃
- Connection Flood
- SYN Flood

また、［ログ出力］で［する］をチェックすると、DoS攻撃防御機能のログをSYSLOGサーバに出力することができます（SYSLOGサーバは　別途ご用意ください）。

3 DoS攻撃が検出されたら、指定したメールアドレスにメールで通知したい場合、［メール通知機能］を設定します。

送信先メールアドレス：送信先のメールアドレスを入力します。

送信元メールアドレス：送信元のメールアドレスを入力します。

メール（SMTP）サーバ：SMTPサーバのIPアドレス、またはドメイン名を入力します。

[DoS攻撃防御設定] 全ての接続／相手先に適用されます	
DoS攻撃防御	◎する ○しない
ログ出力	◎する ○しない
メール通知機能	
送信先メールアドレス	name1@xxxx.ne.jp
送信元メールアドレス	name2@xxxx.ne.jp
メール（SMTP）サーバ	192.168.0.100

4 ［オプション］欄にコマンドを入力して、以下の防御機能を設定することができます。

※{ }で囲まれている部分はパラメータです。パラメータの区切りには、半角スペースを入力してください。

※［オプション］欄で以下の防御機能を利用する設定を行っても、［DoS 攻撃防御設定］の［DoS 攻撃防御］で［する］を選択しなければ有効になりません。

ICMP フラッディング保護機能	
コマンド	ip dos icmpflood mode {on｜off}
機能	ICMP フラッディング保護機能を利用するかどうかの設定
説明	ICMP フラッディング保護機能を利用するかどうか設定します。 この機能により防御できるのは、Ping Flood です。
パラメータ	**on** 利用する off 利用しない
コマンド	ip dos icmpflood echo {number}
機能	ICMP echo request パケット数の設定
説明	ICMP echo request パケット数がこの値を超えると、フラッディングブロックタイム（☞ P.13）が経過するまで、その IP アドレスからの ICMP echo request パケットが破棄されます。
パラメータ	number ICMP echo request パケット数（10～50） （購入時設定：**30**）

TCP インコンプリートセッション保護機能	
コマンド	ip dos incomplete mode {on｜off}
機能	TCP インコンプリートセッション保護機能を利用するかどうかの設定
説明	この機能により SYN Flood を防御することができます。
パラメータ	**on** 利用する off 利用しない
コマンド	ip dos incomplete session high {session}
機能	上限 インコンプリートセッション数の設定
説明	この値を超えるハーフオープン状態のセッションが検出されると、ポート番号に関わらず、すべての TCP セッションが遮断されます。
パラメータ	session インコンプリートセッション数の上限（1～300） （購入時設定：**300**）
コマンド	ip dos incomplete session low {session}
機能	下限 インコンプリートセッション数の設定
説明	TCP インコンプリートセッション保護機能により TCP セッションが遮断された後、ここで設定した値までハーフオープン状態のセッション数が減少したら、セッションを再開します。
パラメータ	session インコンプリートセッション数の下限（1～250） （購入時設定：**250**）

TCP/UDP 非アクティブセッション保護機能	
本製品では、常にTCP/UDP 非アクティブセッション保護機能がONになっています。 この機能では、非アクティブ状態のセッション数をカウントし、非アクティブセッション数が設定された上限値を超えると、そのセッションを遮断します。 これにより、以下の攻撃に対応できます。 ・Connection Flood　・リロード攻撃 ・UDP Flood	
コマンド	ip dos inactive session high {session}
機能	上限 非アクティブセッション数の設定
説明	非アクティブセッション数がこの値を超えると、そのセッションは遮断されます。
パラメータ	session　非アクティブセッション数の上限（1～250） （購入時設定：**250**）
コマンド	ip dos inactive session low {session}
機能	下限 非アクティブセッション数の設定
説明	非アクティブセッション保護機能によりセッションが遮断された後、ここで設定した値まで非アクティブセッション数が減少したら、セッションを再開します。
パラメータ	session　非アクティブセッション数の下限（1～200） （購入時設定：**200**）

同一ホストインコンプリート、非アクティブセッション保護機能	
コマンド	ip dos host incomplete mode {on｜off}
機能	同一ホストインコンプリート、非アクティブセッション保護機能を利用するかどうかの設定
説明	この機能を利用すると、同一IPアドレスからのハーフオープン状態で非アクティブなセッションがチェックされます。 これにより、同一ホストからの下記の攻撃に対応できます。 ・SYN Flood　・リロード攻撃 ・Connection Flood　・UDP Flood
パラメータ	**on**　利用する off　利用しない
コマンド	ip dos host incomplete time {time}
機能	インコンプリート、非アクティブセッション検出時間の設定
説明	ここで設定した時間ごとに、インコンプリート、非アクティブセッションがチェックされます。
パラメータ	time　インコンプリート、非アクティブセッション検出時間（50～5000ミリ秒） （購入時設定：**300**ミリ秒）
コマンド	ip dos host incomplete session {session}
機能	同一インコンプリート、非アクティブセッション数の設定
説明	この値を超える、ハーフオープン状態、または非アクティブTCPセッションとUDPセッションが検出されると、そのIPアドレスからのセッションは遮断されます。 その後、フラッディングブロックタイム（☞ 次ページ）で指定した時間を経過した時点で、そのホストとのセッションが再開されます。
パラメータ	session　インコンプリートセッション数（1～50） （購入時設定：**10**）

同一ホストフラグメンテーション保護機能		
コマンド	ip dos host fragment mode {on｜off}	
機能	同一ホストフラグメンテーション保護機能を利用するかどうかの設定	
説明	この機能を利用すると、同一IPアドレスからの断片化されたパケットがチェックされます。これにより、同一ホストからのFragment Floodに対応できます。	
パラメータ	**on** off	利用する 利用しない
コマンド	ip dos host fragment time {time}	
機能	フラグメンテーション検出時間の設定	
説明	ここで設定した時間ごとに、同一IPアドレスからの断片化されたパケットがチェックされます。	
パラメータ	time	フラグメンテーション検出時間（10～60000ミリ秒） （購入時設定：**10000**ミリ秒）
コマンド	ip dos host fragment packet {packet}	
機能	同一ホスト フラグメンテーションパケット数の設定	
説明	この値を超える、断片化されたパケットが検出されると、そのホストからのセッションは遮断されます。 その後、フラッディングブロックタイム（☞下記）で指定した時間を経過した時点で、そのホストとのセッションが再開されます。	
パラメータ	packet	フラグメンテーションパケット数（1～150） （購入時設定：**30**）

フラッディングブロックタイム		
コマンド	ip dos blocktime {time}	
機能	フラッディングブロックタイムの設定	
説明	フラッディング攻撃が防御され、セッションが遮断されたとき、何秒間遮断するかを設定します。	
パラメータ	time	ブロックタイム（60～30000秒） （購入時設定：**300**秒）

（設定例1）ICMPフラッディング保護機能を利用し、ICMP echo requestパケット数を40、フラッディングブロックタイムを400秒にする場合

```
ip dos icmpflood mode on
ip dos icmpflood echo 40
ip dos blocktime 400
```

（設定例2）TCPインコンプリートセッション保護機能を利用し、下限セッション数を20、上限セッション数を80にする場合

```
ip dos incomplete mode on
ip dos incomplete session low 20
ip dos incomplete session high 80
```

（設定例3）同一ホストインコンプリート、非アクティブセッション保護機能を利用し、セッション数を20、検出時間を600にする場合

```
ip dos host incomplete mode on
ip dos host incomplete session 20
ip dos host incomplete time 600
```

（設定例４） 同一ホストフラグメンテーション保護機能を利用し、パケット数を20、検出時間を5000にする場合

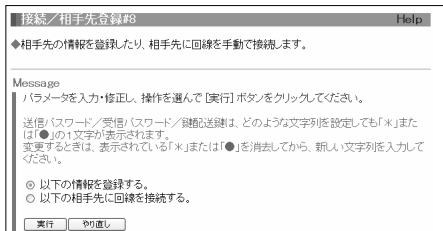
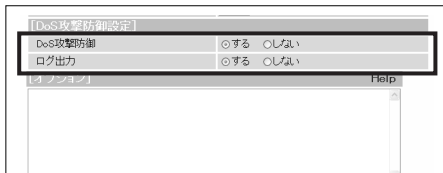
ip dos host fragmentation mode on
ip dos host fragmentation packet 20
ip dos host fragmentation time 5000

5 ［設定］ボタンをクリックします。

すべての接続先に対して、設定した内容が有効になります。
接続した相手先ごとに、DoS攻撃防御機能のON/OFFを設定したい場合は、次ページの手順に従ってください。

接続相手先ごとに、DoS攻撃防御機能のON/OFFを設定する

購入時の設定では、［セキュリティ設定］画面で行ったDoS攻撃防御機能の設定は、すべての接続先に対して有効になります。
接続相手先によって、DoS攻撃防御機能を無効にしたい場合は、以下の手順で設定を変更します。

1 詳細設定ページの［接続/相手先登録］で、設定したい接続先番号のページを開きます。

2 導入時の設定では、［DoS攻撃防御設定］の［DoS攻撃防御］/［ログ出力］で、［する］が選択されています。［しない］を選択すると、その接続相手先に対して、DoS攻撃防御機能/ログ出力機能がそれぞれ無効になります。

3 ［以下の情報を登録する］を選択して、［実行］ボタンをクリックします。

その相手先に対する設定が有効になります。

電話機からの直接設定モード、設定禁止モードを使う

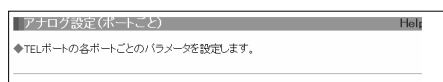
電話機からの設定機能に、次の２つのモードが追加されました。

- フックボタンを押さなくても設定できます。これを「直接設定モード」と呼びます。
- 指定した TEL ポートからの設定を禁止できます。これを「設定禁止モード」と呼びます。

※ フックボタンを押して設定する従来のモードは「フッキング利用モード」と呼びます。
※ 直接設定モードでは、フックボタンを押さなくても設定できるようになりますが、フックボタンを押して設定する（フッキング利用モードと同じ手順で設定する）ことも可能です。

これらのモードを切り替えたいときは、[アナログ設定］ページの［オプション］欄にコマンドを入力します。

直接設定モード、設定禁止モード、フッキング利用モードを切り替える

1 詳細設定ページの［アナログ設定］→［ポートごと］をクリックして、[アナログ設定（ポートごと)］画面を開きます。

2 ［オプション］欄をクリックして、次のコマンドを入力します。

※{ }で囲まれている部分はパラメータです。パラメータの区切りには、半角スペースを入力してください。

書式	analog setup {port mode}
パラメータ	port = 1 ～ 2　ポート番号 mode　モード off　電話機からの設定機能を使わない（設定禁止モード） normal　電話機からの設定機能を、「フッキング利用モード」で使う **direct**　電話機からの設定機能を、「直接設定モード」で使う

（例）TEL ポート２の電話機を、設定禁止モードにするとき

3 ［設定］ボタンをクリックします。

◇ AT コマンドでもモードを切り替えられます

ATコマンド	AT#Ur=n
パラメータ	r=1～2　ポート番号 n=0　電話機からの設定を行わない（設定禁止モード） n=1　電話機からの設定を「フッキング利用モード」で行う n=**2**　電話機からの設定を「直接設定モード」で行う

直接設定モードで設定する手順

※従来のフッキング利用モードで設定する手順は、以下のとおりです。

1. 設定ポートの電話機の受話器を上げる（オフフック）
2. フックボタンを押す（フッキング）
3. #1 ボタンを押す
4. 設定コードとパラメータを入力
5. 最後に＃ボタンを押す

直接設定モードの場合は、以下の手順で設定します。

1 設定ポートの電話機の受話器を上げます。（オフフック）

2 ＊ 1 ボタンを押します。

フッキング利用モードで「フッキング→#1」と操作した場合と同じ状態に移行します。

3 設定コードとパラメータを入力します。

4 # ボタンを押します。

設定が有効になります。引き続き設定したいときは、手順３～４を繰り返します。

直接設定モードで、アナログクイック設定（☞ 次ページ参照）を行う手順

使用頻度の高い設定コードを、まとめて一度に設定できる「アナログクイック設定」の場合は、次の手順で設定します。

1 設定ポートの電話機の受話器を上げます。（オフフック）

2 ＊6 ボタンを押します。

フッキング利用モードで「フッキング→#6」と操作した場合と同じ状態に移行します。

3 クイック設定コード、パラメータを入力します。

4 # ボタンを押します。

設定が有効になります。

引き続きクイック設定コードを入力したいとき：#6 →クイック設定コード・パラメータ→ #
引き続き通常の設定コードを入力したいとき　：#1 →クイック設定コード・パラメータ→ #

電話機からまとめて設定する（アナログクイック設定）

■アナログクイック設定とは

電話機に関する設定のうち、比較的使用頻度の高いものに次の設定があります。

設定内容	設定コード
着信ポート	52 （AT コマンド @ K）
ポート接続機器	32 （AT コマンド @ E）
擬似フレックスホン	63 （AT コマンド @ O）
話中着信	62 （AT コマンド @ N）

これらの設定コードの特定の組み合わせを、1 つのコードで一度に設定することができます。
これを「アナログクイック設定」と呼びます。

例えば、「ポート 1 のみで着信、ナンバー・ディスプレイ、擬似キャッチホンを使用する」という場合、通常の設定コードでは、TEL ポート 1 の電話機から以下の 4 種類を入力する必要があります。
（例） 5201、3211、631、62011

アナログクイック設定で上記と同じ設定をするには「03」を入力するだけで済むので便利です。

なお、アナログクイック設定専用の設定コードを「クイック設定コード」と呼びます。

■アナログクイック設定は、設定を行った電話機のポートに対して有効です

受話器を上げて（オフフックして）設定した電話機のポートに対して設定が行われます。
例えば、TEL ポート 2 の設定を変更したい場合は、TEL ポート 2 に接続した電話機から設定してください。

クイック設定コードは、次の 4 種類です

<table>
<tr><th>クイック設定コード</th><th>機　　能</th></tr>
<tr><td>00
（省略形 0）</td><td>受話器を上げた（オフフックした）ポートの、以下の設定を初期化します

<table>
<tr><th>設定内容</th><th>設定コード</th></tr>
<tr><td>着信ポート</td><td>52 （AT コマンド @ K）</td></tr>
<tr><td>ポート接続機器</td><td>32 （AT コマンド @ E）</td></tr>
<tr><td>擬似フレックスホン</td><td>63 （AT コマンド @ O）</td></tr>
<tr><td>話中着信</td><td>62 （AT コマンド @ N）</td></tr>
</table>

例えば、ポート 1 の電話機から操作した場合、次のように設定されます。
・ダイヤルイン登録番号 0 でかかってきた電話は、すべてのポートで着信
・ポート 1 の接続機器は FAX 機能付き電話、ナンバー・ディスプレイ機能は使用しない
・ダイヤルイン登録番号 0、ポート 1 の電話は、擬似キャッチホンを使用しない
※同等の AT コマンド
　ポート 1 の電話機から設定した場合：　AT@K0=3@E1=10@O0@N01=0@B
　ポート 2 の電話機から設定した場合：　AT@K0=3@E2=10@O0@N02=0@B</td></tr>
</table>

01 （省略形 1）	**受話器を上げた（オフフックした）ポートのみで着信、ナンバー・ディスプレイを使用する** 例えば、ポート１の電話機から操作した場合、次のように設定されます。 ・ダイヤルイン登録番号０でかかってきた電話は、ポート１で着信 ・ポート１の接続機器はFAX機能付き電話、ナンバー・ディスプレイ機能を使用する ※同等のATコマンド ポート１の電話機から設定した場合：　AT@K0=1@E1=11@B ポート２の電話機から設定した場合：　AT@K0=2@E2=11@B
02 （省略形 2）	**受話器を上げた（オフフックした）ポートのみで着信、擬似キャッチホンを使用する** 例えば、ポート１の電話機から操作した場合、次のように設定されます。 ・ダイヤルイン登録番号０でかかってきた電話は、ポート１で着信 ・ダイヤルイン登録番号０、ポート１の電話は、擬似キャッチホンを使用する ※同等のATコマンド ポート１の電話機から設定した場合：　AT@K0=1@O1@N01=1@B ポート２の電話機から設定した場合：　AT@K0=2@O1@N02=1@B
03 （省略形 3）	**受話器を上げた（オフフックした）ポートのみで着信、ナンバー・ディスプレイ、擬似キャッチホンを使用する** 例えば、ポート１の電話機から操作した場合、次のように設定されます。 ・ダイヤルイン登録番号０でかかってきた電話は、ポート１で着信 ・ポート１の接続機器はFAX機能付き電話、ナンバー・ディスプレイ機能を使用する ・ダイヤルイン登録番号０、ポート１の電話は、擬似キャッチホンを使用する ※同等のATコマンド ポート１の電話機から設定した場合：　AT@K0=1@E1=11@O1@N01=1@B ポート２の電話機から設定した場合：　AT@K0=2@E2=11@O1@N02=1@B

設定の手順

1 設定ポートの電話機の受話器を上げます。（オフフック）

2 フックボタンを押してから、#6ボタンを押します。

※購入時の設定では、電話機からの設定機能が直接設定モードに設定されています。〈☞P.15〉
この場合、フックボタンを押さずに＊６ボタンを押す方法でも設定できます。

3 設定コード（00～03のいずれか）を入力します。確認音（ピッ）が聞こえます。

※ここで省略形（０～３のいずれか）を入力すると、確認音は鳴りません。

4 ＃を押します。設定音（ピー）が聞こえたら、設定完了です。

One Point!

◇ 引き続きアナログクイック設定をしたいとき

引き続き、連続してクイック設定コードを入力することができます。
#6 を押してから行ってください。

（例） フッキング利用モードのとき ： フックボタン→#6 → 01（1つめ）→ # → #6 → 03（2つめ）→#

直接設定モードのとき ： ＊6 → 01（1つめ）→ # → #6 → 03（2つめ）→#

◇ 引き続き、通常の設定コードを入力したいとき

引き続き、通常の設定コードを入力することができます。
#1 を押してから行ってください。

（例） フッキング利用モードのとき ：

フックボタン→#6 → 01（クイック設定コード）→ # → #1（通常のコードへ）→ 5212（通常の設定コード）→ # → 4310300001234（通常の設定コード）→ #

直接設定モードのとき：

＊6 → 01（クイック設定コード）→ # → #1（通常のコードへ）→ 5212（通常の設定コード）→ # → 4310300001234（通常の設定コード）→ #

◇ 省略形で設定するとき

クイック設定コードには、先頭の0を省略した省略形があります。
次のように設定できます。

（例） フッキング利用モードのとき ： フックボタン→#6 → 3 → #
省略形（省略形の後、確認音は鳴りません）

直接設定モードのとき ： ＊6 → 3 → #
省略形（省略形の後、確認音は鳴りません）

■お問い合わせ先

本製品について技術的なご質問、または製品のアップグレードに関するご質問は、お買い上げの販売代理店、小売店、またはMNテクニカルセンタまでお問い合わせください。

MNテクニカルセンタ

TEL : 0570－055－128（NTT 一般電話、携帯電話用）
03－5550－8420（PHS、およびNTT以外の電話用）
FAX : 0570－056－128

※9:40～17:50（土・日・休日・年末年始は除く）
※FAXは24時間受け付けております。

■ホームページのご案内

株式会社エヌ・ティ・ティ エムイーのホームページで、製品のサポート情報などを提供しています。

MN128-SOHO ホームページ

◎ 株式会社エヌ・ティ・ティ エムイー「MN128 Information」
http://www.ntt-me.co.jp/mn128/

※記載の商品名、会社名は、各社の商標または登録商標です。